UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/453,509	12/03/1999	ANTHONY BEVERINA	8594-001-64	2741

7590 04/20/2004

Supervisor Patent Prosecution
PIPER RUDNICK LLP
1200 Nineteenth Street, N.W.
Washington, DC 20036-2412

EXAMINER	
BRODA, SAMUEL	
ART UNIT	**PAPER NUMBER**
2123	23

DATE MAILED: 04/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

7

Office Action Summary	Application No.	Applicant(s)
	09/453,509	BEVERINA ET AL.
	Examiner	Art Unit
	Samuel Broda	2123

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 March 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 November 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This communication is in response to:

(1) Applicants' Amendment received 24 March 2003; and

(2) Applicants' Declaration of Anthony F. Beverina and Bryan S. Ware Pursuant to 37 C.F.R. § 1.131 (the "Declaration") received 24 March 2003.

In the Amendment, claims 1, 4, 7, and 10 were amended; claims 1-12 are pending.

In the Declaration, Applicants swear behind the publication date 5 October 1999 of the Veatch et al reference ("An Airport Vulnerability Assessment Methodology"). This reference was used in the prior rejection of the claims under Section 103(a).

1.1 The Declaration filed on 24 March 2003 is sufficient to overcome the Veatch et al reference.

Claim Rejections - 35 U.S.C. § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2.1 Claims 1-2, 4, 7-8, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over:

(a) Anonymous, "SAVI: Systematic Analysis of Vulnerability to Intrusion," Volume 1, SAND89-0926, Sandia National Laboratories, December 1989 (publication available from www.ntis.gov)("Sandia")(prior art previously submitted to Applicants), in view of:

(b) Anonymous, "General Airport Assessment Plan," Science Applications International Corporation, Contract Number: DTFA03-97-C-00036 (November 1997)("SAIC")(reference purchased by the Federal Aviation Administration through a public procurement process described below in Section 2.13).

2.2 Regarding claims 1 and 7, Sandia teaches the "Systematic Analysis of Vulnerability to Intrusion" ("SAVI") software that operates on PCs running DOS. The SAVI software permits a user to model the following characteristics: (1) target; (2) threat; (3) facility; and (4) protection systems, in order to calculate a set of probability of interruption estimates corresponding to "the probability that the response force will interrupt the adversaries prior to completion of their mission." See Sandia, pages A-1 through A-4. A personal computer running SAVI would include a memory, input device, and processor.

Sandia further teaches that the calculation of the probability of non-detection (corresponding to a likelihood of a successful delivery or a probability that a terrorist successfully reaches the target) can be made using the SAVI software based on the worst-case estimates for the individual elements in the model. See pages A-20 through A-21.

The SAVI software models threat vectors corresponding to terrorists possessing equipment and explosives, and attacking while: (1) on foot; (2) in a land vehicle; and (3) in an

aircraft or helicopter. See page A-19. For each site model, the SAVI software ranks and lists the most vulnerable path scenarios. See page A-26. Corresponding to the limitations appearing in Applicants' claims 1 and 7, the SAVI software determines an accessibility of a site by determining a threat vector which is a most likely threat vector by which the weapon will be delivered to the delivery point and the likelihood of a successful delivery based on the model. The SAVI software also provides suggestions for reducing path vulnerability when the software determines that no critical detection point exists on the path and that the probability of interruption equals zero. See pages A-26 through A-29.

However, the SAVI software does not appear to explicitly determine the probability that a terrorist attack will occur, and does not appear to explicitly calculate a risk based at least partially on the accessibility and probability.

SAIC teaches an airport vulnerability assessment methodology that models a relative risk for each threat-target combination. See SAIC, pages 8-9 Section "4.1 Overview." According to SAIC:

> . . . The methodology is applied in a logical, stepped fashion that considers the threat, target identification, aggressor types, malevolent acts of concern, and consequences of a successful malevolent act. Algorithms are used that analyze potential consequences, relative importance of targets to the aggressor, and security vulnerability levels to arrive at a relative risk for each threat and target combination. Countermeasures are then developed to minimize the risk and the methodology is re-applied to determine the risk reduction achieved.

Specifically, SAIC teaches the modeling of a real risk as the product of a target importance ("TI") that includes a consequence value, and a product of two probabilities "(1-LA) (1-LS)" corresponding to the probability that a terrorist attack will occur. See page 11 Section "4.6 Relative Risk." Therefore, SAIC teaches the calculation of a risk based on at least partially on the accessibility and probability that a terrorist act will occur.

According to SAIC, the factor (l-LS) "is proportional to the likelihood that an aggressor will be successful, given an attempt has been made." Page 12 paragraph 1. This factor corresponds to one minus the probability of interruption as calculated by the SAVI software.

2.3 Regarding claims 1 and 7, it would have been obvious to one of ordinary skill in the art at the time of Applicants' invention to incorporate the path vulnerability analysis of the SAVI software into the relative risk calculations taught by SAIC, because the resulting combination would provide more accurate risk calculations and aid in the development of countermeasures to reduce the risk of terrorist attack.

2.4 Regarding claims 2 and 8, SAIC teaches calculation of risks using consequence calculations. See pages 10-11 Section "4.3 Consequences."

2.5 Regarding claims 4 and 10, SAIC teaches preparation of reports indicating probability, accessibility, and relative risk. See pages C-9 and C-12.

2.6 Claims 3 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandia, in view of SAIC, and further in view of Swiatek et al, "SAIC Science and Technology Trends II: Crisis Prediction Disaster Management", pp. 1-13 (June 1999)(paper available at:

http://www.saic.com/products/simulation/cats/VUPQPV4R.pdf)
(prior art previously supplied to Applicants).

2.7 Regarding claims 3 and 9, the combination of Sandia and SAIC teaches calculation of risks using consequence calculations. However, the combination of Sandia and SAIC does not appear to explicitly teach the calculating consequences using a consequence calculator plug-in.

Swiatek et al teaches the "Consequences Assessment Tool Set" ("CATS") software that operates on Pentium PCs running Windows and incorporates a "suite of hazard, casualty, and damage estimation modules to estimate and analyze effects due to natural phenomena, such as hurricanes and earthquakes, and technological disasters, such as terrorist incidents, involving weapons of mass destruction, and industrial accidents." Abstract, page 1 paragraph 1.

The CATS system also includes a "Technological Hazards" software portion that simulates effects due to nuclear, biological, and chemical weapons releases and includes risk calculations based on accessibility and probability. See page 7 column 1 "Technological Hazards". This software portion is separated into plug-in modules; according to Swiatek et al at page 7 column 1:

> . . .While various codes exist that can perform the calculations, the main difficulty with existing NBC hazard products is the lack of a common architecture for the creation of input and output files and the ability to perform analysis for results of multiple models within a common frame of reference. CATS has solved these problems through the

formation of a graphic user interface (GUI) that directly links to the NBC modules utilized, enabling ease of use and analysis in a common geographical information system.

2.8 Regarding claims 3 and 9, it would have been obvious to one of ordinary skill in the art at the time of Applicants' invention to incorporate the plug-in features of the NBC models used in the CATS software into the combination of the SAVI software and the assessment methodology of SAIC, because the resulting software would permit easier analysis using multiple consequence models.

2.9 Claims 5 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandia, in view of SAIC, and further in view of:

(a) Baker et al, "Access Features - Bomb Blast", March 1998 (web page available at: http://www.ncsa.uiuc.edu/News/Access/Stories/BombBlast/indexBB.html)(the "Intro Web Page")(prior art previously supplied to Applicants), and

(b) Baker et al, "Visualization of Damaged Structures", March 1998 (web page available at: http://archive.ncsa.uiuc.edu/Vis/Publications/damage.html)(the "Publication")(prior art previously supplied to Applicants).

In the rejections below, the Intro Web Page supplies the added limitation found in the claims and the Publication supplies the necessary motivation to combine the Intro Web Page with the other references are used in the rejections.

Regarding claims 5 and 11, the combination of Sandia and SAIC does not appear to explicitly teach the display of a three dimensional representation of the most likely threat vector.

The Intro Web Page at page 1 teaches the visualization of structures damaged by terrorist bomb blasts.

According to the Publication at page 3, "the researchers were particularly interested in seeing the progress of the blast's shock front as it hit and went over the top of the building." Because bomb damage can be asymmetric, the researchers also used the three dimensional aspects of the simulation to position the observation point at various views and examine the propagation of the shock front and the subsequent building response.

2.10 Regarding claims 5 and 11, it would have been obvious to one of ordinary skill in the art at the time of Applicants' invention to incorporate the three dimensional blast viewing features of the system of the Intro Web Page with the features of the SAVI software system, and the assessment methodology of SAIC, because such a system would permit the user to better visualize the potential consequences of threat vectors corresponding to explosives placed in buildings.

2.11 Claims 6 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandia, and SAIC, and further in view of Castillo et al, "Modeling Probabilistic Networks of Discrete and Continuous Variables", Journal of Multivariate Analysis, Vol. 64 Issue 1, pp. 48-65 (January 1998)(prior art previously supplied to Applicants).

Regarding claims 6 and 12, the combination of Sandia and SAIC does not appear to explicitly teach the use of risk calculations using Bayesian networks. Castillo et al teaches the use of Bayesian networks to model networks of discrete and continuous variables.

According to Castillo et al, use of Bayesian networks with a set of conditional distributions is preferable to specifying a joint probability distribution when the number of nodes is large. See page 49 paragraph 2. Castillo et al illustrates use of a Bayesian network to model the damage assessment of reinforced concrete structures. See pages 50-57. Use of a Bayesian network permits estimation of the uncertainty propagating through the network (see pages 59-62) and permits sensitivity analysis through parameter modification (see pages 63-64).

2.12 Regarding claims 6 and 12, it would have been obvious to one of ordinary skill in the art at the time of Applicants' invention to incorporate the Bayesian network modelling techniques of Castillo et al with the features of the SAVI software system, and the assessment methodology of SAIC, because such a system would permit uncertainty propagation estimation and sensitivity analysis.

2.13 Claims 1, 4, 7, and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over:

(a) Anonymous, "SAVI: Systematic Analysis of Vulnerability to Intrusion," in view of:

(b) Lazarick, "Airport Vulnerability Assessment – An Analytical Approach," IEEE 32nd Annual International Carnahan Conference on Security Technology, pp. 40-46 (October 1998).

2.14 Regarding claims 1 and 7, Sandia teaches the "Systematic Analysis of Vulnerability to Intrusion" ("SAVI") software that operates on PCs running DOS. The SAVI software permits a user to model the following characteristics: (1) target; (2) threat; (3) facility; and (4) protection systems, in order to calculate a set of probability of interruption estimates

corresponding to "the probability that the response force will interrupt the adversaries prior to completion of their mission." See Sandia, pages A-1 through A-4. A personal computer running SAVI would include a memory, input device, and processor.

Sandia further teaches that the calculation of the probability of non-detection (corresponding to a likelihood of a successful delivery or a probability that a terrorist successfully reaches the target) can be made using the SAVI software based on the worst-case estimates for the individual elements in the model. See pages A-20 through A-21.

The SAVI software models threat vectors corresponding to terrorists possessing equipment and explosives, and attacking while: (1) on foot; (2) in a land vehicle; and (3) in an aircraft or helicopter. See page A-19. For each site model, the SAVI software ranks and lists the most vulnerable path scenarios. See page A-26. Corresponding to the limitations appearing in Applicants' claims 1 and 7, the SAVI software determines an accessibility of a site by determining a threat vector which is a most likely threat vector by which the weapon will be delivered to the delivery point and the likelihood of a successful delivery based on the model. The SAVI software also provides suggestions for reducing path vulnerability when the software determines that no critical detection point exists on the path and that the probability of interruption equals zero. See pages A-26 through A-29.

However, the SAVI software does not appear to explicitly determine the probability that a terrorist attack will occur, and does not appear to explicitly calculate a risk based at least partially on the accessibility and probability.

Lazarick teaches a set of airport vulnerability assessment methodologies that includes modeling a relative risk. These assessment methodologies were developed by contractors and tested at 15 airports, organized through a competitive procurement process through the Federal Aviation Administration ("FAA"), with six contractors eventually involved in a bidder's conference. See pages 41-42.

Specifically, Lazarick teaches the modeling of a real risk as a function of a vulnerability assessment, an asset valuation, and a likelihood of threat attempt corresponding to the probability of terrorist attack. The resulting risk analysis is used to formulate and implement countermeasures. See Fig. 1. According to Lazarick at page 40 "Abstract," such a methodology, part of the "Airport Vulnerability Assessment Project," " . . . uses automation, analytical methods and tools to evaluate vulnerability and risk, and to analyze cost/benefits in a more quantitative manner."

2.15 Regarding claims 1 and 7, it would have been obvious to one of ordinary skill in the art at the time of Applicants' invention to incorporate the path vulnerability analysis of the SAVI software into the risk calculations taught by Lazarick that calculate a relative risk based at least partially on the accessibility and probability, because the resulting combination would provide a more quantitative manner to perform cost/benefit analysis.

2.16 Regarding claims 4 and 10, reports generated by the contractors for the FAA inherently contain data corresponding to probability, accessibility, and relative risk.

2.17 Claims 5 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandia, in view of Lazarick, and further in view of:

(a) Baker et al, "Access Features - Bomb Blast" (the "Intro Web Page"), and

(b) Baker et al, "Visualization of Damaged Structures" (the "Publication").

In the rejections below, the Intro Web Page supplies the added limitation found in the claims and the Publication supplies the necessary motivation to combine the Intro Web Page with the other references are used in the rejections.

Regarding claims 5 and 11, the combination of Sandia and Lazarick does not appear to explicitly teach the display of a three dimensional representation of the most likely threat vector. The Intro Web Page at page 1 teaches the visualization of structures damaged by terrorist bomb blasts.

According to the Publication at page 3, "the researchers were particularly interested in seeing the progress of the blast's shock front as it hit and went over the top of the building." Because bomb damage can be asymmetric, the researchers also used the three dimensional aspects of the simulation to position the observation point at various views and examine the propagation of the shock front and the subsequent building response.

2.18 Regarding claims 5 and 11, it would have been obvious to one of ordinary skill in the art at the time of Applicants' invention to incorporate the three dimensional blast viewing features of the system of the Intro Web Page with the features of the SAVI software system, and the assessment methodology of Lazarick, because such a system would permit the user to better

visualize the potential consequences of threat vectors corresponding to explosives placed in buildings.

2.19 Claims 6 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sandia, and Lazarick, and further in view of Castillo et al, "Modeling Probabilistic Networks of Discrete and Continuous Variables."

Regarding claims 6 and 12, the combination of Sandia and Lazarick does not appear to explicitly teach the use of risk calculations using Bayesian networks. Castillo et al teaches the use of Bayesian networks to model networks of discrete and continuous variables.

According to Castillo et al, use of Bayesian networks with a set of conditional distributions is preferable to specifying a joint probability distribution when the number of nodes is large. See page 49 paragraph 2. Castillo et al illustrates use of a Bayesian network to model the damage assessment of reinforced concrete structures. See pages 50-57. Use of a Bayesian network permits estimation of the uncertainty propagating through the network (see pages 59-62) and permits sensitivity analysis through parameter modification (see pages 63-64).

2.20 Regarding claims 6 and 12, it would have been obvious to one of ordinary skill in the art at the time of Applicants' invention to incorporate the Bayesian network modelling techniques of Castillo et al with the features of the SAVI software system, and the assessment methodology of Lazarick, because such a system would permit uncertainty propagation estimation and sensitivity analysis.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to Applicants' disclosure. Reference to Timm, U.S. Patent 5,440,498, is cited as teaching a method for evaluating security of protected facilities including probability calculations of detecting intrusion and neutralizing the intrusion.

Reference to Draper et al, U.S. Patent 6,254,394, is cited as teaching an area weapons effect simulation system that determines the extent of injuries and damage sustained during a simulated battle.

Reference to Barnes, WO 99/23443 published 14 May 1999, is cited as teaching a knowledge based automatic threat and weapon assignment using calculation of a threat index.

Reference to Anonymous, "The Air Force Antiterrorism/Force Protection (AT/FP) Program Standards, Air Force Instruction 31-210 (August 1999), is cited as teaching terrorist threat levels as a product of factors including targeting.

Reference to Anonymous, "Installation Force Protection Guide," United States Air Force (1997), is cited as teaching performing vulnerability assessments.

Reference to Anonymous, "Combating Terrorism: Threat and Risk Assessments Can help Prioritize and Target Program Investments," General Accounting Office, Report NSIAD-98-74 (April 1998), is cited as teaching a risk assessment matrix based on probability of occurrence and severity level.

Reference to Anonymous, "Hazard Analysis of Commercial Space Transportation," Federal Aviation Administration, Executive Summary and pages 9-1 through 9-27 (October 1995)(paper available at: http://ast.faa.gov/files/pdf/hazard.pdf), is cited as teaching a measure of risk as a function of a probability, hazard, and vulnerability.

4. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Samuel Broda, whose telephone number is (703) 305-1026. The Examiner can normally be reached on Mondays through Fridays from 8:00 AM – 4:30 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, Kevin Teska, can be reached at (703) 305-9704. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the group receptionist, whose telephone number is (703) 305-3900.

SBroda

SAMUEL BRODA, ESQ.
PRIMARY EXAMINER